IN THE CLAIMS

1. (Original) A method of discouraging unauthorized use of a software program, the method comprising the steps of:

configuring the software program in accordance with a software aging process such that one or more files generated by the program are at least partially encrypted using a first cryptographic key associated with a current time interval for which the files are generated; and

providing periodic updates of the software program to a legitimate user of the software program, a given one of the periodic updates including at least a second cryptographic key associated with a time interval subsequent to the current time interval.

2. (Original) The method of claim 1 wherein at least a subset of the periodic updates do not provide any alteration of the functionality of the program but instead discourage piracy of the program through alteration of the cryptographic key used to at least partially encrypt outputs generated by the program.

3. (Original) The method of claim 1 wherein the files generated by the program for the current time interval and at least partially encrypted using the first cryptographic key are readable only by programs having a corresponding decryption key.

4. (Original) The method of claim 3 wherein the first cryptographic key and the corresponding decryption key comprise a common symmetric cryptographic key used for both encryption and decryption.

5. (Original) The method of claim 1 wherein the first cryptographic key is computable as a function of the second cryptographic key using a publicly-known one-way function.

6. (Original) The method of claim 1 wherein each file generated by the software program in a given time interval is labeled with an identifier of the time interval.

7. (Original) The method of claim 6 wherein the time interval identifier uniquely identifies a particular cryptographic key that may be used to decrypt an encrypted portion of a file for that interval.

8. (Original) The method of claim 1 wherein the first encryption key is common to each of a plurality of legitimate copies of the software program that have received a corresponding version of the update.

9. (Original) The method of claim 1 further including the step of providing periodic random updates of the software program to one or more illegitimate users, a given one of the random updates including a random number in place of an cryptographic key associated with a correct update.

10. (Original) The method of claim 1 wherein files generated by the software program for a current time interval t using the first cryptographic key are readable only by copies of the program that have received an update corresponding to at least an interval t-δ, where δ is a designated number of time intervals for which compatibility between current and previous versions is desired.

11. (Original) The method of claim 1 wherein at least a subset of the periodic updates are provided to the legitimate user over a network connection established with a distributor of the software program.

12. (Original) The method of claim 1 wherein at least a subset of the periodic updates are provided to the legitimate user in an automatic manner so as not to be apparent to an operator of the software program.

13. (Original) The method of claim 1 wherein the legitimate user is identified as such by a distributor through the use of an identifier associated with one of a number of known legitimate copies of the software program.

14. (Original) An apparatus for discouraging unauthorized use of a software program, the apparatus comprising:

a memory for storing at least a portion of the software program; and

a processor coupled to the memory and operative to execute at least a portion of the software program, wherein the software program is configured in accordance with a software aging process such that one or more files generated by the program are at least partially encrypted using a first cryptographic key associated with a current time interval for which the files are generated;

wherein periodic updates of the software program are provided to a legitimate user of the software program, a given one of the periodic updates including at least a second cryptographic key associated with a time interval subsequent to the current time interval.

15. (Currently amended) A machine-readable medium containing a software program, executable on a digital data processor comprising a processor and a memory, configured in accordance with a software aging process such that one or more files generated by the program are at least partially encrypted using a first cryptographic key associated with a current time interval for which the files are generated, wherein periodic updates of the software program are provided to a legitimate user of the software program, a given one of the periodic updates including at least a second cryptographic key associated with a time interval subsequent to the current time interval, such that the variation of cryptographic keys from one of the intervals to another of the intervals discourages unauthorized use of the software program.